

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-140304

(43)Date of publication of application : 17.05.2002

(51)Int.Cl.

G06F 15/00
 G06F 17/60
 G10K 15/02
 G10L 19/00
 H04Q 7/38
 H04L 9/32
 H04L 12/28

(21)Application number : 2001-028544

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 05.02.2001

(72)Inventor : SAITO TAKESHI

(30)Priority

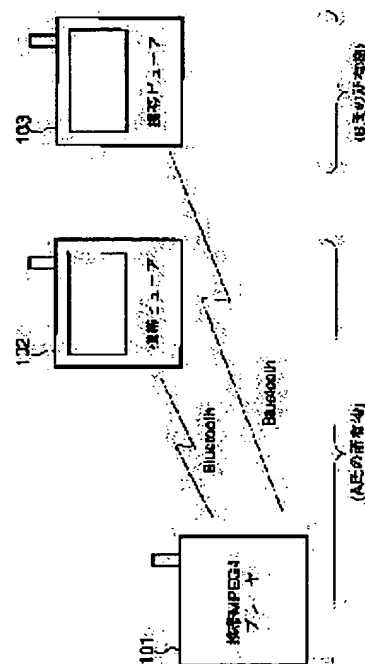
Priority number : 2000252882 Priority date : 23.08.2000 Priority country : JP

(54) RADIO COMMUNICATION SYSTEM, TRANSMITTER, RECEIVER, AND CONTENTS DATA TRANSFER METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a radio communication system which can actualize safe copyright protection even in a radio environment.

SOLUTION: An authenticating and key exchanging procedure of a radio link layer network is carried out between a portable MPEG4 player 101 which sends MPEG4 data whose copyright should be protected and a portable viewer 102 which receives, decodes, and displays the data from the player 101 and when the procedure is successfully followed, an authenticating and key exchanging procedure of DTCP is carried to between the player 101 and viewer 102 by using a cipher communication using a cipher key that the player 101 and viewer 102 shares, and when the authenticating and key exchanging procedure is successfully completed, the data are transferred safely from the player 101 to the viewer 102 by using the cipher communication using the cipher key that the player 101 and viewer 102 shares.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-140304
(P2002-140304A)

(43) 公開日 平成14年5月17日 (2002. 5. 17)

(51) Int.Cl. ⁷	識別記号	F I	テームト* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 C 5 B 0 8 5 3 3 0 B 5 J 1 0 4 3 3 0 F 5 K 0 3 3 3 0 2 E 5 K 0 6 7
17/60	3 0 2	17/60	
G 1 0 K 15/02		G 1 0 K 15/02	

審査請求 未請求 請求項の数15 O L (全 14 頁) 最終頁に続く

(21) 出願番号	特願2001-28544 (P2001-28544)	(71) 出願人	000003078 株式会社東芝 東京都港区芝浦一丁目1番1号
(22) 出願日	平成13年2月5日 (2001. 2. 5)	(72) 発明者	斉藤 健 神奈川県川崎市幸区小向東芝町1番地 株 式会社東芝研究開発センター内
(31) 優先権主張番号	特願2000-252882 (P2000-252882)	(74) 代理人	100058479 弁理士 鈴江 武彦 (外6名)
(32) 優先日	平成12年8月23日 (2000. 8. 23)		
(33) 優先権主張国	日本 (J P)		

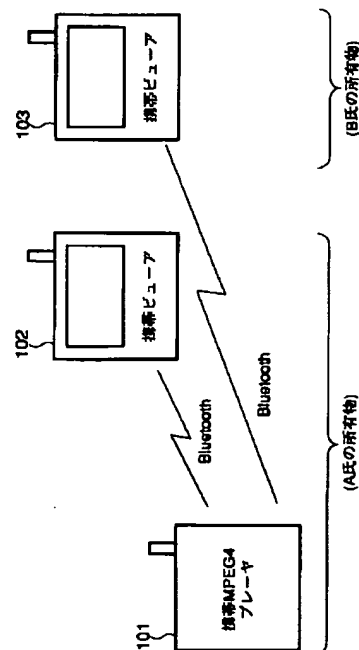
最終頁に続く

(54) 【発明の名称】 無線通信システム、送信装置、受信装置及びコンテンツデータ転送方法

(57) 【要約】

【課題】 無線環境においても安全な著作権保護を実現可能な無線通信システムを提供すること。

【解決手段】 著作権保護すべき M P E G 4 データを送信する携帯 M P E G 4 プレーヤ 1 0 1 と、該プレーヤ 1 0 1 から該データを受信し、デコードして表示する携帯ビューア 1 0 2 との間で、無線リンクレイヤネットワークの認証・鍵交換手続きを行い、この認証・鍵交換手続きの成功によってプレーヤ 1 0 1 とビューア 1 0 2 との間で共有された暗号鍵を用いた暗号通信を利用して、プレーヤ 1 0 1 とビューア 1 0 2 との間で、 D T C P の認証・鍵交換手続きを行い、この認証・鍵交換手続きの成功によってプレーヤ 1 0 1 とビューア 1 0 2 との間で共有された暗号鍵を用いた暗号通信を利用して、プレーヤ 1 0 1 からビューア 1 0 2 へ、安全に該データを転送する。



【特許請求の範囲】

【請求項1】無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおいて、前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行う第1の認証手段と、この第1の認証手段により、前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、この第2の認証手段により、前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする無線通信システム。

【請求項2】無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおいて、前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行う第1の認証手段と、この第1の認証手段により、前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、この第2の認証手段により、前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする無線通信システム。

【請求項3】著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第1の認証手段と、この第1の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、この第2の認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記受信装置へ前記コンテンツデータを送信することを特徴とする無線通信システム。

【請求項4】著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第1の認証手段と、この第1の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、この第2の認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記受信装置へ前記コンテンツデータを転送することを特徴とする送信装置。

【請求項5】前記第2の認証手段または前記第2の鍵交換手続き手段は、前記無線リンクレイヤ上における暗号化通信が介在しなかったことを理由として、前記著作権保護のための認証または前記第2の暗号鍵の共有が失敗した場合に、該失敗の旨および該理由を前記受信装置に通知することを特徴とする請求項3または4に記載の送信装置。

【請求項6】前記コンテンツ・データを記憶するための記憶手段を更に備えたことを特徴とする請求項3ないし5のいずれか1項に記載の送信装置。

【請求項7】前記第1の認証手段による前記認証は、自装置に入力されたPINコードと前記受信装置から通知されたPINコードとが予め定められた一定の関係にある場合に、成立するものであることを特徴とする請求項3ないし6のいずれか1項に記載の送信装置。

【請求項8】前記PINコードは、その都度変化するコード情報、予め定められたコード情報、ユーザの身体から採取した身体情報、またはユーザの属性に関する属性情報の少なくとも一つを含むものであることを特徴とする請求項3ないし7のいずれか1項に記載の送信装置。

【請求項9】著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、自装置が前記送信装置と通信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第1の認証手段と、

この第1の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第2の認証手段と、

この第2の認証手段により、前記送信装置との間で著作権保護のための認証が成功した場合、前記送信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。

【請求項10】著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、

自装置が前記送信装置と通信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第1の認証手段と、

この第1の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第2の認証手段と、

この第2の認証手段により、前記送信装置との間で著作権

権保護のための認証が成功した場合、前記送信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、

前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。

【請求項11】前記コンテンツ・データを表示するための表示手段を更に備えたことを特徴とする請求項9または10に記載の受信装置。

【請求項12】前記第1の認証手段による前記認証は、自装置に入力されたPINコードと前記送信装置から通知されたPINコードとが予め定められた一定の関係にある場合に、成立するものであることを特徴とする請求項9ないし11のいずれか1項に記載の受信装置。

【請求項13】前記PINコードは、その都度変化するコード情報、予め定められたコード情報、ユーザの身体から採取した身体情報、またはユーザの属性に関する属性情報の少なくとも一つを含むものであることを特徴とする請求項9ないし12のいずれか1項に記載の受信装置。

【請求項14】無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおけるコンテンツデータ転送方法であって、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、

この前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有し、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、

この前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有し、

前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とするコンテンツデータ転送方法。

【請求項15】無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおけるコンテンツデータ転送方法であって、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有し、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有し、前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とするコンテンツデータ転送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、無線を介して著作権保護を必要とするデータの転送を行う無線通信システム、送信装置、受信装置及びコンテンツデータ転送方法に関する。

【0002】

【従来の技術】近年、デジタルネットワーク技術の発展が急である。携帯電話やインターネットをはじめとしたネットワーク技術の進歩は、とどまる所を知らず、アプリケーションも、単なる音声通話にとどまらず、多彩なものになってきた。例えば、インターネットにおける音楽配信、あるいは携帯電話に対する無線データ網（i-mode（登録商標）など）を介した音楽配信等は、その典型的な例といえよう。

【0003】一方、デジタル家電と呼ばれる新しい分野も注目を集めている。これは、デジタル技術を用いた新しい家電技術であり、特にデジタル放送の開始や、MD、DVD等のデジタルAV技術を駆使した「デジタルAV家電」の分野は、大変大きな成長が見込まれている。

【0004】これらの分野が融合したと考えられるものが「ネットワーク家電」の分野である。IEEE1394等のネットワークを介してデジタルAVデータ（MP3映像等）をやり取りすることができ、多くのアプリケーションを新たに生み出すことも可能である。

【0005】このような状況で考慮しなければならないのが、著作権保護の問題である。デジタルデータは、加工や蓄積が容易、劣化が無い、等の利点がある反面、「コピーしやすい」等の特徴があり、本来、何らかの対価を支払って購入すべきデジタルデータ（例えば映画や

音楽など）であっても、これを不正にコピーして入手しあるいは譲渡することが可能なわけである。よって、著作権に係るデジタルデータに対する不正行為を未然に防ぐ仕組みを構築することが重要になる。その代表的な例が、IEEE1394におけるDTCP（Digital Transmission Contents Protection）である。これは、IEEE1394上のAVデータの送信装置と受信装置との間で、認証・鍵交換の手順を行ない、AVデータを暗号化・復号化するための暗号鍵を共有した上で、この暗号鍵によって、AVデータを暗号化した上でIEEE1394上を転送することで、第三者による盗聴を防止することができる。また、あらかじめ安全性を保証する機器にしか、上記認証・鍵交換（さらに具体的には、証明書/Certificateの交換）を行なわせないような工夫をすることで、不正な受信装置での不正コピーを未然に防ぐような仕組みが備わっている。

【0006】

【発明が解決しようとする課題】しかしながら、上記の仕組みはIEEE1394やUSBなどの有線ネットワークを前提とした仕組みである。すなわち、無線ネットワークを使ったAVデータの転送を考えた場合、装置間でAVデータを転送することができてしまうため（ケーブルで装置間を接続する必要が無く、単に無線を経由して、送信を指示するだけでAVデータを送信して貰うことが可能であるため）、第三者がコンテンツを傍受することが可能になってしまい、不正行為を防止することができない、と言う問題点があった。

【0007】本発明は、上記事情を考慮してなされたもので、無線環境においても安全な著作権保護を実現可能な無線通信システム、送信装置、受信装置及びコンテンツデータ転送方法を提供することを目的とする。

【0008】

【課題を解決するための手段】本発明は、無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システム／コンテンツデータ転送方法において、前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有し、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有し、前記

無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする。あるいは、前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする。

【0009】本発明は、著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上に、前記受信装置との間の認証を行う第1の認証手段と、この第1の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、この第2の認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記受信装置へ前記コンテンツデータを送信することを特徴とする。あるいは、前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記受信装置へ前記コンテンツデータを転送することを特徴とする。

【0010】本発明は、著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、自装置が前記コンテンツを受信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上に、前記送信装置との間の認証を行う第1の認証手段と、この第1の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第2の認証手段と、この第2の認証手段により、前記送信装置との間で著作権保護のための認証が成功した場合、前記送信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から送信された前記コンテンツデータを受信すること

を特徴とする。あるいは、前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から送信された前記コンテンツデータを受信することを特徴とする。

【0011】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0012】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0013】本発明では、著作権保護すべきコンテンツ・データを送信する送信装置と、該送信装置から著作権保護された該コンテンツ・データを受信する受信装置との間で、無線リンクレイヤネットワークに依存した第1の認証・鍵交換手続きを行い、続いて、著作権保護すべきコンテンツ・データに依存した第2の認証・鍵交換手続きの全部または一部を、第1の認証・鍵交換手続きの成功によって前記送信装置と前記受信装置との間で共有された第1の暗号鍵を用いた暗号通信によって行うので、該第1の認証を成功させることのできる正当な送信装置と受信装置との間でのみ、第2の暗号鍵を用いた暗号通信による該コンテンツ・データの転送を行うことができる。

【0014】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0015】（第1の実施形態）図1に、本実施形態の無線通信システムの構成例を示す。

【0016】図1に示されるように、ソース機器となる携帯MPEG4プレーヤ101と、これに対するシンク機器となる携帯ビューア102とが、ローカルエリア無線ネットワークで接続できる範囲内に位置している（携帯MPEG4プレーヤ101と携帯ビューア102はそれぞれこのローカルエリア無線ネットワークの無線インタフェースを有するものとする）。

【0017】ここで、図1に示されるように、携帯MPEG4プレーヤ101と携帯ビューア102の他に、携帯ビューア103（携帯ビューア102と同様の基本構成とする）も携帯MPEG4プレーヤ101へローカルエリア無線ネットワークで接続できる範囲内に位置している場合を考える。

【0018】すなわち、これら3つの携帯端末が同一の無線LAN（Bluetoothの場合は単一ピコネット）内に存在しており、携帯MPEG4プレーヤからBluetooth経由でどちらの携帯ビューアに対して

もMPEG4映像を転送することができる範囲内に存在しているものとする。そして、携帯MPEG4プレーヤ101と携帯ビューア102は同一人物…A氏とする…の携帯物であり（A氏が対にして使用しようとしているものであり）、携帯ビューア103はA氏とは異なる人物…B氏とする…の携帯物である（A氏が使用しようとしていないものである）とする。なお、ここでは簡単のために携帯ビューア103について考えるが、A氏以外の人物の携帯する携帯ビューアが他に接続範囲内に存在していても携帯ビューア103と同様である。

【0019】また、転送するMPEG4映像（MPEG4データ）は、著作権保護をかけた上で転送すべきものである場合を考える。

【0020】なお、ここでは、ローカルエリア無線ネットワークとしては、Bluetoothを仮定して説明する。Bluetoothは、低コスト、低消費電力などを特徴とする無線LANの一種であり、多くの携帯端末や家電製品などへの搭載が期待されている（例えば、<http://www.bluetooth.com>にて取得可能に開示されている文書に説明が詳しい）。また、以下で用いるBTの表記は、Bluetoothを略したものである。

【0021】以下、図1のような状況において、携帯MPEG4プレーヤ101から携帯ビューア102に対してのみMPEG4映像を転送可能（携帯ビューア102においてのみ再生、視聴可能）とするための構成について説明する。

【0022】図2に、携帯MPEG4プレーヤ101の内部構造の一例を示す。

【0023】図2に示されるように、携帯MPEG4プレーヤ101は、Bluetoothの物理レイヤ処理を実行するBluetoothインタフェース（I/F）処理部11、Bluetoothのデータリンクレイヤ処理を実行するbluetooth通信処理部12を備えている。

【0024】Bluetoothは、そのスペック内に「Bluetooth Security」なる認証、鍵交換、データ暗号化の方式が規定されている。つまり、Bluetoothというリンクレイヤ方式内部に、データ暗号化や、認証・鍵交換の方式が定められている。携帯MPEG4プレーヤ101は、この処理部（BT認証・鍵交換手続き（データのやり取り）を行うためのBT認証・鍵交換処理部13、PINコードを入力するためのPINコード入力部14、送信すべきデータを暗号化し、受信したデータを復号化するためのBTレイヤ暗号・復号化部15）を、内部に持っている。Bluetoothレベルの認証は、PINコードと呼ばれるコード（例えば、数桁の数字やパスワード、あるいは指紋情報などの身体情報、等）の照合によって行われる。

【0025】この他、携帯MPEG4プレーヤ101は、MPEG4 AVデータを蓄積しておくMPEG4ストレージ19、これをBluetoothパケットに変換するパケット化部18、さらにMPEG4のデータを暗号化して転送するための著作権保護レイヤ（アプリケーションレベル）の処理部（DTCP認証・鍵交換手続き（データのやり取り）を行うためのDTCP認証・鍵交換部16、送信すべきデータを暗号化するためのDTCP暗号化部17）を内部に持つ。

10 【0026】ここで、DTCPとは、Digital Transmission Contents Protectionの略で、IEEE1394やUSBなどでデファクトスタンダードとなっている著作権保護の方式である。著作権保護が必要なAVデータ（例えば、AVデータに著作権保護が必要か否かを示す情報が付加されている）に対して、送信装置と受信装置との間で、認証・鍵交換を行ない、AVデータを暗号化して転送する仕組みが備わっている（例えば、<http://www.dttla.com>にて取得可能に開示されている文書に説明が詳しい）。

20 【0027】図3に、携帯ビューア102（103）の内部構造の一例を示す。

【0028】図3に示されるように、携帯ビューア102は、Bluetoothインタフェース（I/F）処理部21およびbluetooth通信処理部22、Bluetoothレベルの認証・鍵交換や暗号化の処理部（BT認証・鍵交換手続き（データのやり取り）を行うためのBT認証・鍵交換処理部23、PINコードを入力するためのPINコード入力部24、送信すべきデータを暗号化し、受信したデータを復号化するためのBTレイヤ暗号・復号化部25）、AVデータ（アプリケーションレベル）の認証・鍵交換や暗号化を行う処理部（DTCP認証・鍵交換手続き（データのやり取り）を行うためのDTCP認証・鍵交換部26、受信したデータを復号化するためのDTCP復号化部27）を備えている。

【0029】また、携帯ビューア102は、BluetoothパケットをMPEG4データにリアセンブリするパケットリアセンブリ部28、MPEG4データをデコードするMPEG4デコーダ29、MPEG4データを表示するためのディスプレイ30を備えている。

40 【0030】図4に、Bluetoothレイヤの認証手順の概要を示す。各々の装置（携帯MPEG4プレーヤ、携帯ビューア）では、PINコードが入力される（ステップS1）。なお、PINコードは、その都度入力する方法や、予め入力して設定しておく方法などがある。両装置は、（BT認証・鍵交換処理部13、23により）Bluetoothレイヤの認証手順を行う（ステップS2）。両装置間でPINコードを交換し、それらのPINコードが一致して認証に成功すれば（ステッ

ブS3)、bluetoothレイヤの鍵交換手順が行われ、鍵共有に成功する(ステップS4)。この後、(BTレイヤ暗号・復号化部15、25が)共有したbluetoothレイヤの鍵を用いることによって、(DTCP認証・鍵交換部16、26による)DTCP認証・鍵交換を安全に行うことができる。これによって、DTCPの鍵を共有し、MPEG4データの暗号通信が可能になる(DTCP暗号化部17で暗号化し、DTCP復号化部27で復号化することが可能になる)。一方、両装置のPINコードが一致せず認証に失敗すれば(ステップS3)、bluetoothレイヤの鍵交換手順が行われるが、鍵共有に失敗する(ステップS5)。この場合には、bluetoothレイヤの鍵が共有されていないので、たとえ(DTCP認証・鍵交換部16、26による)DTCP認証・鍵交換が動作しても、(間違ったbluetoothレイヤの鍵で復号化を行うことになり)、DTCP認証・鍵交換を成功させることができない(DTCPの鍵を共有することができない)。さらに、DTCP認証・鍵交換が成功していなければ、たとえ(DTCP暗号化部17でDTCPの鍵を用いて)暗号化されたMPEG4データを受信しても、(DTCP復号化部27では正しいDTCPの鍵を知らないの)でその復号化ができない。なお、両装置のPINコードが一致せず認証に失敗した場合には、bluetoothレイヤの鍵交換手順自体を行わないようにしてもよい。

【0031】なお、本実施形態では、両装置のPINコードの値の一致をもって認証の成功としているが、その他、一方のPINコードの値と他方のPINコードの値とが予め定められた一定の関係(例えば、ユーザ属性情報として住所情報の一部を利用する関係、等)にある場合に、認証の成功とするようにしてもよい(なお、両装置のPINコードの値が一致するという関係も、一定の関係の一場合である)。

【0032】ここで、PINコードのバリエーションについて説明する。

【0033】まず、PINコードの入力あるいは設定方法として、種々のバリエーションがある。

【0034】例えば、(1)ユーザがその都度入力する方法、(2)ユーザが予め設定しておく方法、(3)製造者または販売者等が(ユーザが変更できない形で)予め設定しておく方法、(4)上記の(1)～(3)の全部又は一部を併用する方法(例えば、(1)コードと(3)のコードを連結する等)など、種々の方法が考えられる。また、例えば、ユーザが上記の(1)または(2)について適宜選択可能とする方法もある。

【0035】また、PINコードの内容としても、種々のバリエーションがある。

【0036】(1)または(2)の方法の場合、例えば、PINコードをユーザがその都度決定する方法があ

る。また、例えば、一方の装置…例えば携帯MPEG4プレーヤ…内でランダムにパスワードを発生させ、これを該一方の装置側でPINコードとして記憶するとともにユーザに呈示し、これを読み取ったユーザが同一のパスワードを他方の装置…例えば携帯ビューア…に入力する方法もある。また、指紋情報、声門情報、あるいは角膜情報等を用いる方法もある(この場合、それら情報を採取する装置が、携帯MPEG4プレーヤや携帯ビューアに内蔵されているか、または携帯MPEG4プレーヤや携帯ビューアに外部接続可能である必要がある)。

【0037】また、(2)の方法の場合に、携帯MPEG4プレーヤや携帯ビューアに、ユーザ属性情報が登録されているならば、この情報(例えば、ユーザ名、住所、年令、学校名、職業、会社名、部課名、家族名等)に基づいてPINコードを生成する方法もある(ただし、PINコードを生成するもとなる情報は、両装置でPINコードを同一にするような値…例えば同一の値…にしておく必要がある)。

【0038】また、(3)の方法の場合に、製造者または販売者等が、製造時または販売時に、1セットの携帯MPEG4プレーヤや携帯ビューアに同一の乱数を設定しておく方法がある。また、販売者が、販売時に、ユーザの指紋情報等を採取して1セットの携帯MPEG4プレーヤや携帯ビューアに設定しておく方法がある。

【0039】さて、本実施形態の携帯MPEG4プレーヤおよび携帯ビューアは、「正当な対になるプレーヤ/ビューア間では、AVデータ転送アプリが正常に稼動する」、「正当な対でないプレーヤ/ビューア間では、AVデータ転送アプリが正常に稼動しない(ビューアでAVデータは正常に再生できない)」という状況を実現している。例えば、同一人物が所有する携帯MPEG4プレーヤおよび携帯ビューアを正当な対とした場合に、自分の所有する携帯MPEG4プレーヤからのデータが自分の所有する携帯ビューアで再生されるが、自分の所有する携帯MPEG4プレーヤからのデータが他人の所有する携帯ビューアで再生されず、かつ、自分の所有する携帯ビューアで他人の所有する携帯MPEG4プレーヤからのデータが再生されない、という環境を実現できる。

【0040】つまり、一般的に、インタフェースが無線の場合には、プレーヤから出力された電波は必ずと一定範囲内のビューアにて受信し得る状態にさらされるので、これをビューア側から見ると、各々の携帯ビューアは、正当な対になる携帯プレーヤにも、それ以外の携帯プレーヤにも、アクセスする(送信を指示する)ことが可能であり得てしまう。ここで、著作権保護レイヤにおいては、両方の装置(送信側の装置と受信側の装置)がDTCPコンプライアント(DTCP準拠)なデバイスであれば、認証鍵交換は、どちらの場合にも成立し得てしまう。つまり、著作権保護レイヤでは、相手側の装置が正当な対になる装置であるのか、それ以外の装置であ

るのかについて区別することができない。そこで、相手側の装置が正当な対になる装置であるのか、それ以外の装置であるのかを区別するために、本実施形態では、Bluetoothレベルの認証を用いるようにしている。

【0041】すなわち、Bluetoothレベルでの認証・鍵交換が成立すると、それは「正当な対になる装置である」と判断し、アプリケーションレベル(DTCPレベル)の認証・鍵交換に移行する。Bluetoothレベルでの認証・鍵交換が成立しないと、それは「正当な対になる装置ではない」と判断して、アプリケーションレベル(DTCPレベル)の認証・鍵交換に移行することを拒否することとする。

【0042】これは、Bluetoothレベルの認証・鍵交換のレベルで認証が成立すれば、その両装置(送信装置と受信装置)が正当な対になる装置であると認識することができることによる。すなわち、Bluetoothレベルの認証が、「両装置(送信装置と受信装置)に、同一のPINコード(例えば、数桁の数字やパスワード、あるいは指紋情報等)を入力することができる」あるいは「両装置(送信装置と受信装置)に、同一のPINコードが設定されている」ことを根拠として、この値を用いて認証手続きを行なっていることから、この結果、両装置は正当な対であると推測・認識するのに十分である(正当な対でない装置に入力されたPINコード同士が偶然一致する確立はきわめて小さい)と考えられるためである。

【0043】例えば、同一人物が所有する(あるいは占有する)携帯MPEG4プレーヤと携帯ビューアが正当な対をなすものとした場合に、A氏が自分の持つ携帯MPEG4プレーヤと携帯ビューアに同一のPINコード(パスワード)を入力することはできるが、B氏がこれと同じPINコード(パスワード)を推測して自分の持つ携帯ビューアに入力することは大変な困難が伴うので、MPEG4プレーヤと携帯ビューアで入力されたPINコードが同一ならば同一人物が所有する正当な対であると判定し、MPEG4プレーヤと携帯ビューアで入力されたPINコードが相違するならば異なる人物が所有する正当でない対であると判定することができる。また、PINコードに指紋情報等を用いる場合には、B氏がA氏と同じPINコード(指紋情報等)を自分の持つ携帯ビューアに入力することは、A氏の指紋情報等を盗用でもできないかぎり、不可能である。

【0044】ここで、図1の携帯MPEG4プレーヤ101と携帯ビューア102との間のやり取りおよび携帯MPEG4プレーヤ101と携帯ビューア103との間のやり取りを例にとって説明する。

【0045】図5に、正当な対になるA氏の携帯MPEG4プレーヤ101と携帯ビューア102との間で行われるシーケンスの一例を示す。

【0046】なお、図5においてリンクレイヤによる暗号化および復号化に関する記載は自明であるので省いてある。

【0047】この場合、まず、携帯MPEG4プレーヤ101と携帯ビューア102の両装置には、それぞれ、所定のタイミングで(例えば、事前に、あるいは使用時に)、所定の方法によるPINコードの入力がなされる(ステップS11、S12)。ここでは、携帯MPEG4プレーヤ101側で入力されたPINコードの値をxとし、携帯ビューア102側でもPINコードの値として同じ値xが入力されたものとする。両装置のPINコードの値が一致することで、続くBluetoothレイヤ・認証手順を成功裡に終了させることができる。

【0048】続いて、Bluetoothレイヤ・リンクキー共有手順を行って(ステップS13)、それに引き続き認証・鍵交換に用いるリンクキーK1の値を共有する(ステップS14、S15)。

【0049】続いて、Bluetoothレイヤの認証手順を行う(ステップS16)。この場合は、PINコードの共有により、認証が成立する。

【0050】続いて、Bluetoothレイヤ鍵交換手順を行って(ステップS17)、Bluetoothレイヤ暗号鍵Kbtの値を共有する(ステップS18、S19)。

【0051】これによって、Bluetoothレイヤにおいて、両装置間で、任意のデータの交換を暗号化の上(他人に盗聴、書き換えができないようにして)行うことができるようになる。

【0052】次に、携帯MPEG4プレーヤ101と携帯ビューア102の両装置は、DTCP(著作権保護レイヤ)の認証・鍵交換を行うフェーズに移る。ここで、両装置は、DTCPの認証・鍵交換の手順の全部又は一部を、Bluetoothレベルの暗号化を行った上で行うと好ましい。このようにすることで、DTCP認証・鍵交換を、「(Bluetoothレベルでの認証・鍵交換に成功した)正当な対をなす装置間でのみ」行なう(完遂する)ことを保証できるようになり、ひいては「正当な対をなす(例えば、同一人物の携帯する)装置間でのみ、著作権保護レイヤ(DTCP)の認証・鍵交換が成立する」、「正当な対をなす(例えば、同一人物の携帯する)装置間でのみ、著作権保護レイヤ(DTCP)レベルの暗号鍵の共有が出来る」ということが可能になる。

【0053】さて、携帯MPEG4プレーヤ101と携帯ビューア102の両装置は、DTCP認証・鍵交換を、Bluetoothレイヤレベルの暗号化を利用して行ない(ステップS20)、両装置間でのDTCPレイヤ(著作権保護レイヤ)の暗号鍵Kcの共有が達成される(ステップS21、S22)。

【0054】これを受けて、送信側装置である携帯MP

EG4プレーヤ101は、送信するAVコンテンツ(MPEG4データ)を暗号鍵Kcで暗号化して(ステップS23)、受信側装置である携帯ビューア102に送信する(ステップS24)。携帯ビューア102は、DTCPレベルの暗号鍵Kcを共有しているため、この暗号化コンテンツを復号化することが出来、MPEG4データのとりだしを行うことができる。すなわち、携帯ビューア102は、受信した暗号化コンテンツをDTCPレベルの暗号鍵Kcで復号化し(ステップS25)、ディスプレイに表示する。

【0055】これに対して、同じBluetoothピコネット内にいる別の受信装置は、DTCPレベルの認証・鍵交換を行っていないため、暗号鍵Kcを共有しておらず、このデータを再生することはできない。これを以下に説明する。

【0056】図6に、正当な対にならないA氏の携帯MPEG4プレーヤ101とB氏の携帯ビューア103との間で行われるシーケンスの一例を示す。

【0057】まず、携帯MPEG4プレーヤ101と携帯ビューア103の両装置では、それぞれ、所定のタイミングで(例えば、事前に、あるいは使用時に)、所定の方法によるPINコードの入力がなされる(ステップS31、S32)。

【0058】しかし、この場合、前述のように携帯MPEG4プレーヤ101側で入力されたPINコードの値をxとした場合に、携帯ビューア103側で入力されたPINコードの値x'がxに一致することはないか、または確率的に極めて低い。すなわち、例えば、PINコードをユーザが手入力する場合には、両装置は、異なる人物が携帯する装置であるため、両装置に同一のPINコードが入力されることは非常に難しい。また、正当な対をなす装置に予め固有のPINコードを書き込んでおく場合には、この例ではA氏の携帯MPEG4プレーヤ101とB氏の携帯ビューア103の両装置は正当な対をなす装置ではないものとしているので、両装置のPINコードが一致することはない。

【0059】よって、たとえBluetoothレイヤ・リンクキー共有手順を行って(ステップS33)、それに引き続き認証・鍵交換に用いるリンクキーの値の共有を試みても(ステップS34、S35)、PINコードが一致していないので、これに基づいて生成された携帯MPEG4プレーヤ101側のリンクキーK1と、携帯ビューア103側のリンクキーK1'とは一致せず、リンクキーの共有は失敗に終わることになる。

【0060】従って、続くBluetoothレイヤ認証手順を行っても(ステップS36)、これは失敗に終わることになる。この結果、これに続くBluetoothレイヤ鍵交換手順が行なわれない。

【0061】そして、Bluetooth暗号化が成立しないため、DTCP認証・鍵交換手順に入ることがで

きず、DTCPの認証・鍵交換を成功裡に行うことができない。すなわち、送信側の携帯MPEG4プレーヤ101は、もし、受信側の携帯ビューア103より、DTCPレベルの認証・鍵交換の要求が来たとしても(ステップS37)、これがBluetoothレベルの暗号化がなされない形で送信されてきた場合には、これを拒否する(ステップS38)。よって、正当な対でない

(例えば、所有者が異なる)装置同士では、著作権保護レベルの認証・鍵交換が成立せず、著作権を保護すべきAVデータの転送は、行なえないこととなる。

【0062】なお、ステップS38の拒否メッセージを相手に通知する際に、その拒否の理由(リンクレイヤすなわちBluetoothレイヤの暗号化がかかっていないため、あるいはBluetoothレイヤの認証が行われていないため)を併せて通知するようにしてもよい。これは、相手が正当なもの(例えば同一所有者のもの)である場合に、Bluetoothレイヤの認証・鍵交換の実行を促すものとなる。

【0063】なお、以上では、携帯MPEG4プレーヤにMPEG4データが蓄積されているものとしているが、MPEG4データを外部から取得するものであってもよいし、符号化する前のソースデータが蓄積されていてMPEG4コードを備えてMPEG4を生成してもよいし、ソースデータを外部から取得しMPEG4コードでMPEG4を生成してもよい。また、MPEG4映像(MPEG4データ)以外のデータの送受信にも本発明はもちろん適用可能である。

【0064】また、以上では、送信装置1台に対して受信装置を1台とする通信を前提として説明したが、送信装置から複数台の受信装置へのデータ転送も可能である。この場合には、例えば、図5のシーケンスにおいて、携帯MPEG4プレーヤと各々の携帯ビューアとの間で、暗号鍵Kcの共有までの手順を、逐次行って、認証・鍵交換に成功した全装置で暗号鍵Kcを共有するようにしてもよい。この結果、携帯MPEG4プレーヤがAVコンテンツを暗号鍵Kcで暗号化して送信すれば、暗号鍵Kcの共有に成功した正当な携帯ビューアは、暗号化コンテンツを復号化し、表示することができる。なお、この場合に、送信装置ごとに、あるいはコンテンツごとに、送信装置から同時にデータ転送可能な受信装置の台数の上限を設定可能にしてもよい。

【0065】(第2の実施形態)第1の実施形態では、著作権保護レイヤ(DTCP)の認証・鍵交換の手順の全部又は一部を、Bluetoothレイヤの暗号・復号化部を通して行うものであった。これに対して、第2の実施形態は、MPEG4データ(AVデータ)の転送そのものについても、Bluetoothレイヤの暗号・復号化部を通して行うようにしたものである。

【0066】本実施形態では、第1の実施形態と相違する部分を中心に説明する。

10

20

30

40

50

【0067】図7に、第1の実施形態における図2に対応する本実施形態の携帯MPEG4プレーヤ101の内部構造の一例を示す。また、図8に、第1の実施形態における図3に対応する本実施形態の携帯ビューア102(103)の内部構造の一例を示す。いずれも、第1の実施形態に対して、BTレイヤ暗号・復号化部がBluetooth通信処理部とDTC P暗号化部との間に接続されている点が相違する。

【0068】また、図9に、第1の実施形態における図5のシーケンス例に対応する本実施形態におけるシーケンスの一例を示す。

【0069】なお、図9においてリンクレイヤによる暗号化および復号化に関する記載は自明であるので省いてある。

【0070】これは、第1の実施形態に対して、AVデータが、DTC Pレイヤ(著作権保護レイヤ)の暗号鍵KcとBluetoothレイヤ暗号鍵Kbtによって多重に暗号化されている点が相違する。すなわち、携帯MPEG4プレーヤは、送信する著作権保護すべきAVコンテンツを暗号鍵Kcで暗号化した後に、暗号鍵Kbtで暗号化する。また、携帯ビューア102は、受信した暗号化されたAVコンテンツを暗号鍵Kbtで復号化した後に、暗号鍵Kcで復号化する。

【0071】本実施形態は、第1の実施形態と比べ、DTC Pの認証・鍵交換手順及びデータ暗号化・復号化の両方について、Bluetooth暗号化をかけて行うため、処理速度は遅くなるものの、装置構成は単純なものにすることが可能となる(例えば、DTC P処理を単一のLSIで行なっている場合には、全ての入出力を、Bluetoothレイヤ暗号・復号化部を経由させることで、構成が単純になる)。

【0072】なお、本実施形態においても、正当な対でない(例えば、異なる人物の)装置間では、両装置に同一のPINコードが入力されることは非常に難しいため、Bluetoothレイヤ認証手順が失敗してしまう。よって、これに引き続くBluetoothレイヤ鍵交換手順が行なわれない。よって、この後、Bluetooth暗号化が成立しないため、DTC P認証・鍵交換手順に入ることができず、DTC Pの認証・鍵交換を成功裡に行うことができない。よって、正当な対でない(例えば、所有者が異なる)装置同士では、著作権を保護すべきAVデータの転送は、第1の実施形態と同じく、行なえないこととなる。

【0073】なお、本実施形態では、無線LANとして、Bluetoothを例に説明してきたが、802.11無線LANや、WECA方式、HomeRF方式の無線LAN等、リンクレイヤレベルで認証・鍵交換、暗号化等のセキュリティ機能を持つ無線LANは多い。本発明は、これらの種々の無線LANに適用することが可能である。

【0074】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0075】また、本実施形態は、コンピュータに所定の手段を実行させるための(あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための)プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0076】なお、各実施形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。また、各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。また、各実施形態は、個別装置としての発明、関連を持つ2以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

【0077】従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【0078】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0079】

【発明の効果】本発明では、認証手続きを成功させることのできる正当な装置間でのみ、正しく暗号鍵を共有することができ、正しく暗号鍵を共有することができた装置間でのみ、暗号通信によるデータ転送が可能になる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る無線通信システムの構成例を示す図

【図2】同実施形態に係る携帯MPEG4プレーヤの内部構造の一例を示す図

【図3】同実施形態に係る携帯ビューアの内部構造の一例を示す図

【図4】Bluetoothレイヤの認証手順の概要を説明するためのフローチャート

【図5】正当な対になる携帯MPEG4プレーヤと携帯ビューアとの間で行われるシーケンスの一例を示す図

【図6】正当な対にならない携帯MPEG4プレーヤと

携帯ビューアとの間で行われるシーケンスの一例を示す図

【図7】同実施形態に係る携帯MPEG4プレーヤの内部構造の他の例を示す図

【図8】同実施形態に係る携帯ビューアの内部構造の他の例を示す図

【図9】正当な対になる携帯MPEG4プレーヤと携帯ビューアとの間で行われるシーケンスの他の例を示す図

【符号の説明】

11, 21…Bluetoothインタフェース処理部

12, 22…Bluetooth通信処理部

13, 23…BT認証・鍵交換処理部

* 14, 24…PINコード入力部

15, 25…BTレイヤ暗号・復号化部

16, 26…DTCP認証・鍵交換部

17…DTCP暗号化部

18…パケット化部

19…MPEG4ストレージ

27…DTCP復号化部

28…パケットリアセンブリ部

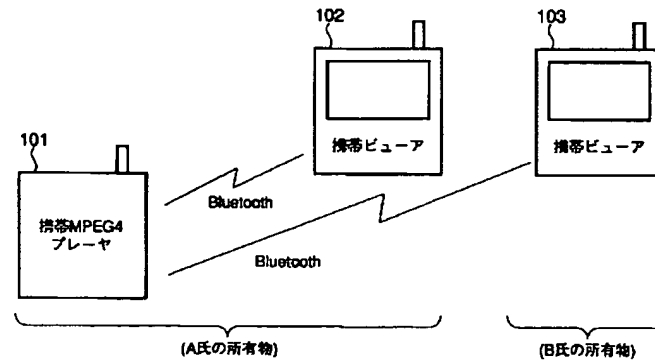
29…MPEG4デコーダ

10 30…ディスプレイ

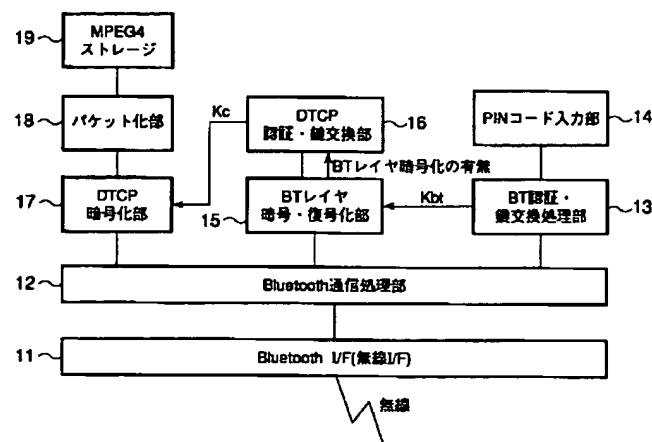
101…MPEG4プレーヤ

* 102, 103…携帯ビューア

【図1】



【図2】



```

graph TD
    30[ディスプレイ] --> 29[MPEG4デコーダ]
    29 --> 28[パケットリアセンブリ部]
    28 --> 27[DTCP復号化部]
    27 -- Kc --> 26[DTCP認証・鍵交換部]
    26 -- "BTレイヤ暗号化の有無" --> 25[BTレイヤ暗号・復号化部]
    25 -- Kbt --> 23[BT認証・鍵交換処理部]
    24[PINコード入力部] --> 23
    23 -- Kbt --> 26
    23 --> 22[Bluetooth通信処理部]
    22 --> 21[Bluetooth I/F(無線I/F)]
    21 -- 無線 --> Antenna[無線]
  
```

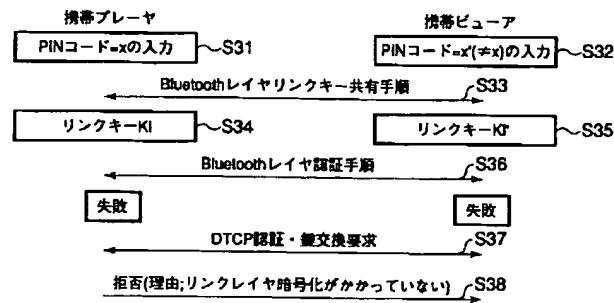
```

graph TD
    S1[PINコードの入力] --> S2[BTレイヤ認証手順]
    S2 --> S3{双方のPINコード一致?}
    S3 -- YES --> S4[Bluetoothレイヤ鍵交換へ]
    S3 -- NO --> S5[認証失敗  
(Bluetoothレイヤ  
鍵交換は行わない)]
  
```

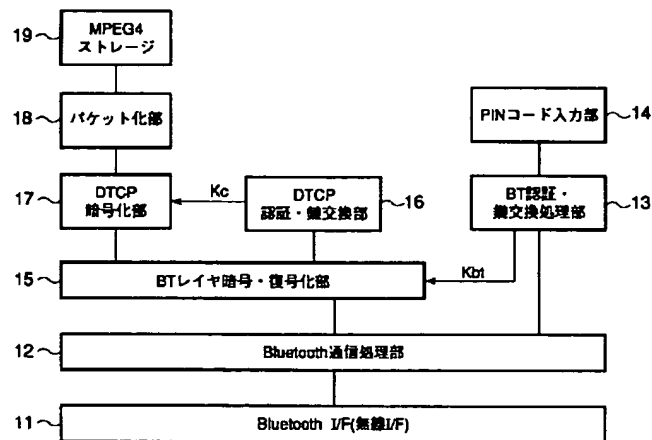
```

sequenceDiagram
    participant P as 携帯プレーヤ
    participant B as 携帯ビューア
    Note over P: PINコード=xの入力
    P->>B: Bluetoothレイヤ リンクキー共有手順
    Note over B: PINコード=xの入力
    B->>P: リンクキー-KIの共有
    Note over P: リンクキー-KIの共有
    P->>B: Bluetoothレイヤ 認証手順
    Note over B: リンクキー-KIの共有
    B->>P: Bluetoothレイヤ 鍵交換
    Note over P: BTレイヤ暗号鍵Kbtの共有
    P->>B: [DTCP認証・鍵交換]Kbt
    Note over B: BTレイヤ暗号鍵Kbtの共有
    B->>P: DTCPレイヤ(著作権保護レイヤ)暗号鍵Kcの共有
    Note over P: DTCPレイヤ(著作権保護レイヤ)暗号鍵Kcの共有
    P->>B: AVコンテンツのKcによる暗号化
    Note over B: DTCPレイヤ(著作権保護レイヤ)暗号鍵Kcの共有
    B->>P: [AVコンテンツ]Kc
    Note over P: AVコンテンツのKcによる暗号化
    P->>B: Kcによる復号化, AVコンテンツの取り出し
  
```

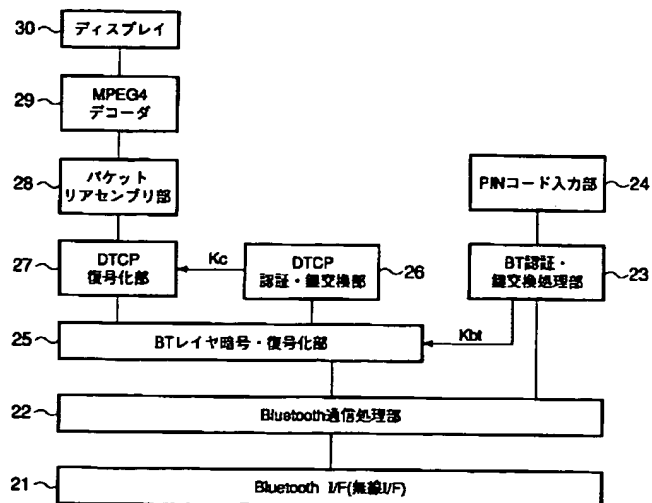
【図6】



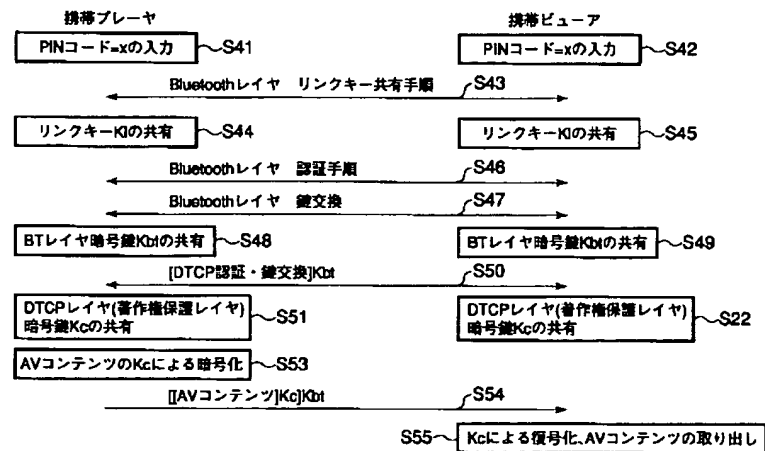
【図7】



【図8】



【図9】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
G 1 0 L 19/00		H 0 4 L 12/28	3 0 0 Z
H 0 4 Q 7/38		G 1 0 L 9/00	N
H 0 4 L 9/32		H 0 4 B 7/26	1 0 9 R
12/28	3 0 0	H 0 4 L 9/00	6 7 3 D
			6 7 5 A

F ターム (参考) 5B085 AA08 AE01 AE04 AE25 AE29
 5J104 AA01 AA07 AA15 JA03 KA01
 KA04 KA16 KA17 NA02 NA05
 5K033 AA08 BA13 BA15 CB14 CC01
 DA19
 5K067 AA32 BB21 DD17 EE02 HH12
 HH24 HH36

【公報種別】 特許法第17条の2の規定による補正の掲載
 【部門区分】 第6部門第3区分
 【発行日】 平成17年10月20日(2005.10.20)

【公開番号】 特開2002-140304(P2002-140304A)
 【公開日】 平成14年5月17日(2002.5.17)
 【出願番号】 特願2001-28544(P2001-28544)
 【国際特許分類第7版】

G 0 6 F 15/00
 G 0 6 F 17/60
 G 1 0 K 15/02
 G 1 0 L 19/00
 H 0 4 Q 7/38
 H 0 4 L 9/32
 H 0 4 L 12/28

【F I】

G 0 6 F	15/00	3 3 0 C
G 0 6 F	15/00	3 3 0 B
G 0 6 F	15/00	3 3 0 F
G 0 6 F	17/60	3 0 2 E
G 1 0 K	15/02	
H 0 4 L	12/28	3 0 0 Z
G 1 0 L	9/00	N
H 0 4 B	7/26	1 0 9 R
H 0 4 L	9/00	6 7 3 D
H 0 4 L	9/00	6 7 5 A

【手続補正書】
 【提出日】 平成17年6月30日(2005.6.30)
 【手続補正1】
 【補正対象書類名】 明細書
 【補正対象項目名】 特許請求の範囲
 【補正方法】 変更
 【補正の内容】
 【特許請求の範囲】
 【請求項1】

無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおいて、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行う第1の認証手段と、

この第1の認証手段により、前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、

この第2の認証手段により、前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする無線通信システム。

【請求項2】

無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおいて、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行う第1の認証手段と、

この第1の認証手段により、前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、

この第2の認証手段により、前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、

前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする無線通信システム。

【請求項3】

著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、

前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第1の認証手段と、

この第1の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、

この第2の認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記受信装置へ前記コンテンツデータを送信することを特徴とする無線通信システム。

【請求項4】

著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、

前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第1の認証手段と、

この第1の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第2の認証手段と、

この第2の認証手段により、前記受信装置との間で著作権保護のための認証が成功した

場合、前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、

前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記受信装置へ前記コンテンツデータを転送することを特徴とする送信装置。

【請求項5】

前記第2の認証手段または前記第2の鍵交換手続き手段は、前記無線リンクレイヤ上における暗号化通信が介在しなかったことを理由として、前記著作権保護のための認証または前記第2の暗号鍵の共有が失敗した場合に、該失敗の旨および該理由を前記受信装置に通知することを特徴とする請求項3または4に記載の送信装置。

【請求項6】

前記コンテンツ・データを記憶するための記憶手段を更に備えたことを特徴とする請求項3ないし5のいずれか1項に記載の送信装置。

【請求項7】

前記第1の認証手段による前記認証は、自装置に入力されたPINコードと前記受信装置から通知されたPINコードとが予め定められた一定の関係にある場合に、成立するものであることを特徴とする請求項3ないし6のいずれか1項に記載の送信装置。

【請求項8】

前記PINコードは、その都度変化するコード情報、予め定められたコード情報、ユーザの身体から採取した身体情報、またはユーザの属性に関する属性情報の少なくとも一つを含むものであることを特徴とする請求項3ないし7のいずれか1項に記載の送信装置。

【請求項9】

著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、

自装置が前記送信装置と通信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第1の認証手段と、

この第1の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第2の認証手段と、

この第2の認証手段により、前記送信装置との間で著作権保護のための認証が成功した場合、前記送信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。

【請求項10】

著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、

自装置が前記送信装置と通信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第1の認証手段と、

この第1の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第2の認証手段と、

この第2の認証手段により、前記送信装置との間で著作権保護のための認証が成功した

場合、前記送信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する第2の鍵交換手続き手段とを備え、

前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。

【請求項11】

前記コンテンツ・データを表示するための表示手段を更に備えたことを特徴とする請求項9または10に記載の受信装置。

【請求項12】

前記第1の認証手段による前記認証は、自装置に入力されたPINコードと前記送信装置から通知されたPINコードとが予め定められた一定の関係にある場合に、成立するものであることを特徴とする請求項9ないし11のいずれか1項に記載の受信装置。

【請求項13】

前記PINコードは、その都度変化するコード情報、予め定められたコード情報、ユーザの身体から採取した身体情報、またはユーザの属性に関する属性情報の少なくとも一つを含むものであることを特徴とする請求項9ないし12のいずれか1項に記載の受信装置。

【請求項14】

無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおけるコンテンツデータ転送方法であって、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、

この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有し、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、

この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有し、

前記無線リンクレイヤ上に設けられた、前記第2の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とするコンテンツデータ転送方法。

【請求項15】

無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおけるコンテンツデータ転送方法であって、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、

この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有し、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、

この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有し、

前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受

信装置へ前記コンテンツデータを転送することを特徴とするコンテンツデータ転送方法。

【請求項 16】

著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、

前記受信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する手続を行う第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う認証手段と、

この認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する手続を行う第2の鍵交換手続き手段とを備え、

前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記受信装置へ前記コンテンツデータを転送することを特徴とする送信装置。

【請求項 17】

著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、

前記送信装置との間で共通の第1の暗号鍵を生成し、この第1の暗号鍵を共有する手続を行う第1の鍵交換手続き手段と、

前記第1の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う認証手段と、

この認証手段により、前記送信装置との間で著作権保護のための認証が成功した場合、前記送信装置との間で共通の第2の暗号鍵を生成し、この第2の暗号鍵を共有する手続を行う第2の鍵交換手続き手段とを備え、

前記第2の暗号鍵に基づき暗号化された暗号化通信路を、前記第1の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。